

ORDER

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

1600.61A

11/03/00

**SUBJ: FOREIGN TRAVEL BRIEFING & CONTACT REPORTING REQUIREMENTS FOR FAA
AND CONTRACTOR EMPLOYEES**

1. PURPOSE. This order establishes security briefing requirements for FAA and contractor employees prior to travel to foreign countries on official and unofficial business, and requirements for reporting certain contacts with foreign nationals. It implements provisions of Order DOT 1640.4D, Classified Information Management, and Presidential Decision Directive (PDD) 12, Security Awareness and Reporting of Foreign Contacts.

2. DISTRIBUTION. This order is distributed to all managers in FAA headquarters, regions, centers, field offices, and facilities.

3. CANCELLATION. Order 1600.61, Defensive Security Briefing Requirements for FAA Employees Traveling to Communist-Controlled Countries, dated November 30, 1982, is canceled.

4. EXPLANATION OF CHANGES. This order:

a. Implements DOT requirements for foreign travel briefings and reporting certain contacts with foreign nationals.

b. Establishes specific time frames for providing the required briefings.

c. Broadens the scope of this order to encompass persons under contract or agreement with the FAA.

d. Changes the title of the order to reflect current dual requirements.

e. Eliminates specific briefing requirements for travel to particular countries and the use of DOT Form 1630-6, Defensive Security Briefing Certificate, which is now obsolete.

5. BACKGROUND.

a. In carrying out the FAA's mission, FAA and contractor employees sometimes travel on agency business to countries whose interests are not entirely in concert with those of the United States (U.S.) or to countries where there are criminal or terrorist threats to their safety. Innocent travel and tourist activities, often perfectly acceptable in the U.S., may be seized upon by other nations as a basis for the arbitrary arrest or detention of travelers, and as a means of embarrassing the travelers and the U.S. All

U.S. Government and contractor employees, regardless of agency, position, or assignment, are of particular interest because of their association with the U.S. and/or awareness or actual knowledge of information that could be used to enhance the military, technological, or economic strength of a foreign country. Even a limited amount of information, whether classified or not, could be combined with information from other sources to the advantage of a foreign country or detriment of the U.S.

b. PDD 12 states that foreign intelligence services (FIS) continue to acquire classified or otherwise sensitive information and recruit personnel believed to have access to such information despite the end of the Cold War and the collapse of the former Soviet Union. These intelligence services are associated with and operate in countries considered friendly to the U.S. as well as countries whose interest is generally considered inimical to those of the U.S. Most FIS cultivate friendships to create an assessment period before actual recruitment or exploitation of a person. The majority of such contacts can appear to be innocent social encounters or requests for “unimportant” information.

c. Terrorist groups, foreign nationals, and private industry can present a threat to FAA and contractor employees through random violence and attempts to obtain FAA sensitive, proprietary, and classified information. Only those who are aware of this threat will recognize when they are being targeted for any purpose and when they are being manipulated toward involvement in intelligence or terrorist activities.

6. AUTHORITY TO CHANGE THIS ORDER. The Associate Administrator for Civil Aviation Security is authorized to issue changes to this order which do not establish or revise policy, delegate authority, or assign responsibility.

7. DEFINITIONS.

a. Defensive Security Briefing. A formal briefing that alerts the recipient to the potential for harassment, exploitation, provocation, capture, or entrapment. The briefing includes information on courses of action helpful in mitigating adverse security and personnel consequences and advice on passive and active measures that personnel should take to avoid becoming targets or inadvertent victims while on foreign travel. (Refer to Director of Central Intelligence Directive 1/20, Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI)).

b. Foreign National. A person who is not a citizen or national of the U.S..

c. Official Travel. Travel performed at the direction of the U.S. Government.

d. Senior Officials of the Intelligence Community (SOIC). The heads of organizations within the Intelligence Community or their designated representatives.

e. Sensitive Compartmented Information (SCI). All intelligence information and material that requires special controls for restricted handling within compartmented channels and for which compartmentation is established.

f. Servicing Security Element (SSE). The organization responsible for providing security services to Washington headquarters, regions, and centers. These elements are the Office of Civil Aviation Security Operations (ACO) in the Washington headquarters, the Civil Aviation Security Divisions in the regions, and at the Aeronautical Center and the Civil Aviation Security Staff at the Technical Center.

g. Unofficial Travel. Travel undertaken by an individual without official, fiscal, or other obligations on the part of the U.S. Government.

8. POLICY.

a. A security briefing is required for each FAA employee prior to his/her departure for any foreign country on official business, unless he/she has received a briefing within 12 months of the date of departure.

b. All FAA and contractor employees shall be made aware, through a security briefing, of situations they could encounter while on travel to foreign countries and of basic defensive measures they can take against these threats. Each person shall conduct himself/herself in such a manner that prevents personal and professional compromise and shall do everything possible to avoid involvement in situations that might embarrass the U.S. and/or the FAA.

9. RESPONSIBILITIES.

a. Associate Administrator for Civil Aviation Security, ACS-1, is responsible for the overall implementation of the provisions of this order and, as necessary, providing updated information for security briefings.

b. Office of Civil Aviation Security Policy and Planning, ACP-1, is responsible for developing policy and guidance to implement DOT requirements for foreign travel briefings and for reporting contacts with foreign nationals and all suspicious contacts.

c. Office of Civil Aviation Security Operations, ACO-1, is responsible for ensuring that SSE's assist supervisors and employees in complying with the provisions of this order and for providing oversight of this program throughout FAA.

d. Director, Office of Civil Aviation Security Intelligence/SOIC, ACI-1, or his/her designee is responsible for notifying each FAA employee with access to SCI when special security briefings are required for travel to a foreign country and for providing these briefings.

e. Service Security Elements are responsible for assisting supervisors, operating offices, and FAA employees in complying with this order.

f. Operating Offices shall ensure all contractor employees, and other persons by agreement with the FAA, who work in or have access to FAA facilities, sensitive information, and/or resources for which they are responsible:

(1) Are made aware of the provisions of this order at least 14 days prior to traveling to a foreign country.

(2) In the case of short-notice (less than 14 days prior to expected departure date) foreign travel, are made aware of the provisions of this order as soon as practicable prior to departure.

(3) Certify in writing that they have been made aware of the provisions of this order by signing and dating the certification found in Appendix 1, Guide for Employees Traveling to Foreign Countries.

(4) Receive a copy of appendix 1 upon request.

g. Supervisors shall ensure that FAA employees:

(1) Are made aware of the provisions of this order at least 14 days prior to traveling to a foreign country.

(2) In the case of short-notice (less than 14 days prior to expected departure date) foreign travel, are made aware of the provisions of this order as soon as practicable prior to departure.

(3) Certify, in writing, that they have been made aware of the provisions of this order by signing and dating the certification form found in appendix 1.

(4) Receive a copy of appendix 1 upon request prior to personal, unofficial travel to a foreign country.

h. Employees shall report to their managers and their SSE any contact with individuals of any nationality who seek illegal or unauthorized access to classified or sensitive information, either while in a foreign country or in the U.S. Employees shall also report to the SSE any concerns they have that they may be the targets of actual or attempted exploitation by a foreign entity.

10. TARGET RECOGNITION.

a. FAA and contractor employees should be aware that an intelligence agency, security service, terrorists, criminals, or a competitor could target them if they are believed to be U.S. citizens and/or knowledgeable of, or carrying information concerning, but not limited to, the following:

(1) Facilities and systems for air navigation and control of air traffic, particularly the capabilities and vulnerabilities of these systems.

(2) How the FAA protects its critical infrastructure, especially from deliberate attempts to disrupt the national airspace system and/or FAA operations.

(3) Technologies that may not be readily available in other countries or on which there are export restrictions.

(4) The FAA's interactions with foreign governments, including proposed agreements, contracts, and other working relationships.

(5) Information a foreign government shares with the FAA in confidence.

(6) FAA support provided to classified or sensitive military operations or law enforcement activities.

(7) Sensitive security information (SSI) as defined in 14 CFR Part 191, Sensitive Security Information.

(8) Intelligence activities, intelligence methods or sources, and communications security (COMSEC) equipment, keying material, and operating procedures.

(9) Classified information or other matters related to the national security.

b. These are indicators of unwarranted interest that each FAA and contractor employee should be familiar with:

(1) Repeated contacts with a foreign national or other individual who is not involved in your business interests or the purpose of your visit, but as a result of invitations to social or business functions, appears at each function. This individual's demeanor may indicate more than just a passing interest in you or your business activities.

(2) Establishment of close social relationships with representatives of a foreign government for business reasons that begin to develop beyond the business level.

(3) Accidental encounters with unknown foreign nationals or other unknown persons who strike up a conversation and want to talk about the U.S., politics, your employment, etc. The individual may try to use other excuses to begin a "friendly" relationship.

(4) Any unauthorized solicitation of classified, sensitive, or proprietary information.

(5) Unusual interest in specific duties, functions, or responsibilities of an individual, position, office, unit, or agency.

(6) Unusual or repeated requests for seemingly "unimportant" information.

(7) Any events that suggest targeting of FAA personnel, facilities, or resources by a FIS or terrorist group.

(8) Any offer to provide you classified or sensitive information.

(9) All information regarding the intentions of terrorist organizations.

(10) All information regarding planned or actual acts of sabotage or subversion.

11. GENERAL SECURITY BRIEFING REQUIREMENTS.

- a. Each FAA and contractor employee must receive a security briefing within 14 days prior to departure for any travel to a foreign country on official business.
- b. Each FAA and contractor employee must receive a security briefing concerning the reporting of certain contacts and incident information annually.
- c. The briefing need not consist of anything other than a reading of Appendix 1, Guide for Employees Traveling to Foreign Countries, which contains the information required for this briefing.
- d. Regional Security Officer will provide security awareness information to those FAA and contractor employees who are permanently assigned to a U.S. diplomatic mission.
- e. Employees are encouraged to check Travel Warnings and Public Announcements and Consular Information sheets issued by the Bureau of Consular Affairs, Department of State, for countries that they plan to visit. This information is available on the State Department's web site, <http://travel.state.gov>, or can be obtained by calling Overseas Citizens Services, 202-647-5225.

12. SPECIAL SECURITY BRIEFING REQUIREMENTS. The Central Intelligence Agency (CIA) grants certain FAA employees access to SCI. Persons granted access to SCI incur a special security obligation and, with the exception of official travel, are discouraged from traveling to countries that pose a threat to SCI and/or SCI indoctrinated personnel. In accordance with Director of Central Intelligence Directive (DCID) 1/20, all SCI holders must notify ACI-1 in writing of all foreign travel. SCI indoctrinated travelers must be alerted to the risks associated with foreign travel. Failure to comply with the following provisions may result in the withdrawal of approval for continued access to SCI and may be considered in determining whether to grant future SCI access approvals.

a. Official Travel. Employees with access to SCI engaging in official travel shall:

- (1) Submit an itinerary in writing to ACI-1 within 14 days prior to the date of travel.
- (2) Attend a Defensive Security and/or a Risk of Capture briefing as determined by ACI-1 within 14 days prior to travel, as necessary.
- (3) Report to ACI-1 any unusual incidents or contacts as described in paragraph 10.

b. Unofficial Travel. Employees with access to SCI engaging in unofficial travel shall:

- (1) Submit an itinerary in writing to ACI-1 within 14 days prior to the date of travel, unless the travel is due to a personal emergency.
- (2) Attend a Defensive Security and/or a Risk of Capture briefing if determined by ACI-1 as necessary.

(3) Be advised that such travel without cognizant SOIC approval may result in the withdrawal of approval for continued access to SCI.

(4) Report to ACI-1 any unusual incidents or contacts as described in paragraph 10.

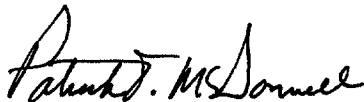
13. CONTACT AND INCIDENT REPORTING REQUIREMENTS.

a. FAA and contractor employees shall report to their SSE any contact with a foreign national that would appear to be an attempt to obtain unauthorized access to classified, sensitive, or proprietary information or technology and/or the possibility of continued contact with such an individual.

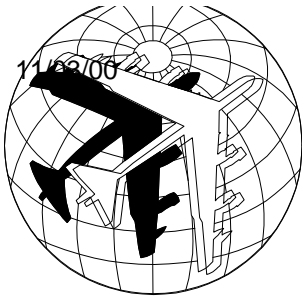
b. SSE's shall review and evaluate all information reported by FAA and contractor employees and report to the Office of Security and Administrative Management (M-40), Office of the Secretary, through the Investigations Division (ACO-300), any facts or circumstances of a reported contact or incident that would appear to meet one of the criteria in paragraph 10a (1) and (2), or 10b.

14. CLASSIFIED INFORMATION. FAA and Contractor employees who need access to classified information during travel outside of the U.S., who need to transfer it outside of the U.S., or who need to send it back to the U.S. from a foreign country, shall follow the requirements and procedures contained in the latest edition of Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information.

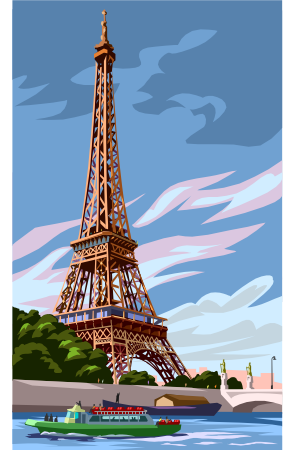
15 - 199. RESERVED.



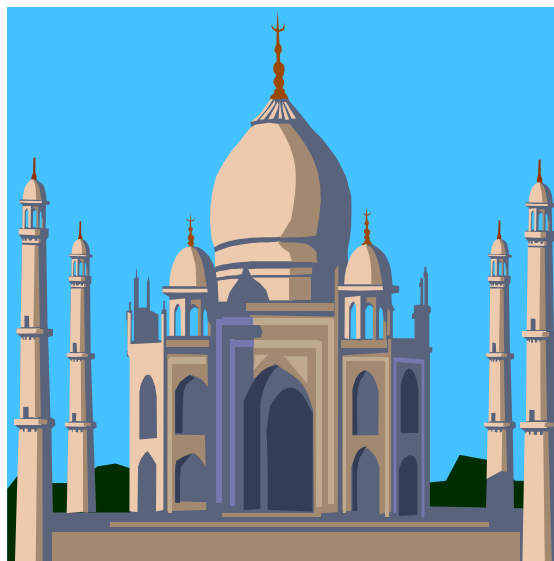
for William S. Davis
Acting Associate Administrator for Civil Aviation Security



1600.61A
APPENDIX 1



GUIDE FOR EMPLOYEES TRAVELING TO FOREIGN COUNTRIES



INDEX

| | |
|--|----|
| SECTION I - INTRODUCTION | 3 |
| SECTION II - PREPARATION | 4 |
| PASSPORT, VISAS, AND DRIVER'S LICENSE | 4 |
| MEDICAL | 5 |
| LUGGAGE AND PACKING | 6 |
| SECTION III - WHILE IN A FOREIGN COUNTRY | 7 |
| GENERAL INFORMATION | 7 |
| LOCAL LAW | 8 |
| PERSONAL SAFETY | 9 |
| ON THE STREET | 9 |
| IN THE HOTEL | 9 |
| USING PUBLIC TRANSPORTATION | 10 |
| WHILE DRIVING | 10 |
| IV - TERRORISM AND INTELLIGENCE TARGETING | 11 |
| TERRORISM | 11 |
| INTELLIGENCE TARGETING | 13 |

SECTION I INTRODUCTION

Millions of U.S. citizens travel abroad each year. Whether foreign travel is for official business, personal business, or pleasure the odds is in your favor that you will have a safe and incident-free trip that is a positive and rewarding experience. However, earthquakes, hurricanes, political upheavals, petty or violent crime or acts of terrorism are only some of the unexpected difficulties that can befall U.S. citizens in all parts of the world.

Planning and good judgment can often prevent problems that range from the inconvenient to the very serious. This booklet outlines security precautions, and offers suggestions and guidance that should help DOT employees avoid difficulties while traveling in foreign countries.

Inform yourself about the countries you will visit. Libraries, bookstores, and travel agencies all have books and brochures. Be alert to the news about the current conditions in these countries, including reports about any controversial political or social issues that may cause unrest. [The Department of State provides current travel information and issues travel warnings when conditions warrant \[www.travel.state.gov\]\(http://www.travel.state.gov\). You may listen to recorded travel advisories, 24 hours a day, on the Department of State's Citizens Emergency Center recording 202-647-5225.](#)

Do not publicize your travel plans. Limit your travel information to the few people who have a need to know. Leave a full itinerary of your travel schedule, hotel phone numbers, and business appointments with your office, a member of your family, or a friend. Establish a point of contact at your office for your family to call in an emergency.

From time to time, all travelers experience frustrations such as overcrowded hotels, rental car nonavailability, overbooked restaurants, and delays in flight schedules. Use common sense and good judgment in your reactions to these situations. Remain calm and do not be excessively critical of the local customs and conditions that you find disagreeable. Do not be surprised if you occasionally encounter anti-American sentiments in some of the foreign countries that you visit; do not become involved in discussions that compare other countries with the United States.

Remember that citizens of other countries will form opinions about America based on the kind of impression you make on them. As an American abroad, you are a symbol of your country.

SECTION II-PREPARATION

A. PASSPORT, VISAS, AND DRIVER'S LICENSE

Be sure you sign your passport and fill in the personal notification data on page 4. If your passport is mutilated or altered in any way, other than changing the personal notification data, it may render the passport invalid and expose you to possible prosecution under Title 22 of the U.S. Code. Check to be sure that your passport is valid and up-to-date and that visas are current for the country of destination. If your passport or visas are not valid, you and everything in your possession may be looked at in depth by host government authorities. If you are carrying documents that are sensitive or proprietary, they will be examined in detail to see if there is anything that would be of interest to the foreign government. If there is, you can be sure that copies will be made. To prevent this: NEVER pack sensitive or proprietary information in your checked luggage. Double envelop the material and hand carry it or send it via the diplomatic pouch well in advance.

Make photocopies of your passport, licenses, credit cards, airline tickets, and any other important documents that you will carry with you. Put copies in both your carry-on and checked luggage. Leave a copy of those documents, along with a list of the serial numbers of your travelers' checks, with someone at your home or office. If the documents are lost or stolen, these records will speed up the replacement process.

If your passport is lost or stolen in the U.S., report it immediately to Passport Services, 1425 K Street, N.W., Department of State, Washington D.C. 20524, or to the nearest passport agency. If it should be lost or stolen abroad report it immediately to the local police and to the nearest U.S. embassy or consulate.

Your passport is the most valuable document you will carry abroad. It confirms your U.S. citizenship. Guard it carefully. When you carry it with you, do not carry it in a handbag or an exposed pocket. Whenever possible, leave your passport in the hotel safe, not in an empty hotel room or packed in your luggage. One family member should not carry all the passports for the entire family.

Your passport is your best form of identification. You will need it to pick up mail or check into a hotel, and U.S. Immigration requires you to prove your citizenship and identity when you are ready to reenter the United States.

You may sometimes be required to leave your passport at the hotel reception desk overnight so local police may check it. This is a normal procedure in some countries and is required by their local laws. If your passport is not returned the following morning, directly report the impoundment to local police authorities and the nearest U.S. embassy or consulate.

Some countries are sensitive to which visa you obtain. If you are traveling on official Government business, a diplomatic or official passport should be obtained; otherwise for personal travel a tourist passport is required. If you travel frequently to countries requiring visas, you may request a 48-page passport at the time you apply. There is no additional charge for the extra pages.

Be aware of your passport's expiration date. Some countries will not permit you to enter and will not place a visa in your passport if the remaining validity is less than 6 months. If you return to the U.S. with an expired passport, you are subject to a fee at the port of entry.

If you plan to rent a car, check to see if you must obtain an international driver's permit for any country that you plan to visit.

B. MEDICAL

Some countries may require international certificates of vaccination against yellow fever and cholera. Typhoid vaccinations are not required for international travel, but are recommended for areas where there is risk of exposure. Smallpox vaccinations are no longer given. Ensure that your measles, mumps, rubella, polio, diphtheria, tetanus, and pertussis immunizations are up-to-date. Some countries require certification from long-term visitors that they are free of the human immuno-deficiency virus (HIV). Generally, this has little bearing on tourists and short-term visitors.

If you go abroad with pre-existing medical conditions, carry a letter from your doctor describing your condition, including information on any prescription medicines you must take. Know the generic names of the drugs. Take plenty of any prescription medication with you, as well as an extra set of eyeglasses or contact lenses. Ensure that all prescription medication is in its original container with the prescription label attached. Pack your medication and eyeglasses in your carry on luggage to ensure it is not lost.

All employees going on temporary duty travel should have medical coverage under the Federal Employees Health Benefits Program or other medical insurance program. This coverage is the primary source of medical benefits while overseas. While on temporary

duty assignment abroad, you are also covered under the Department of State (DOS) Medical Program for payment of medical expenses for inpatient hospital care and related outpatient treatment not covered by your health insurance. This coverage includes hospitalization for illness, injury or medical conditions, which occurs while you are on temporary duty, as well as outpatient care and medical travel related to such hospitalization. Coverage under the program does not include outpatient care that is not related to the hospitalization.

If you become seriously ill while on temporary duty overseas, you must contact the nearest American embassy or consulate. Officials on duty 24 hours a day will provide you the names of reputable physicians and hospitals. If available medical facilities at post are inadequate to treat your condition, the embassy will authorize medical evacuation to the nearest location where suitable medical care can be obtained. Since most hospitals in foreign countries do not take credit cards and most will not honor U.S. medical insurance plans, the embassy will normally provide a promissory note to the hospital as form of payment.

C. LUGGAGE AND PACKING

Safety begins when you pack. To avoid being a target, dress conservatively. A flashy wardrobe or one that is too casual can mark you as a tourist. As much as possible, avoid the appearance of affluence.

Always try to travel light, if you do, you can move quickly and will be more likely to have a free hand. You will also be less likely to set your luggage down, leaving it unattended.

Carry the minimum amount of valuables necessary for your trip and plan a place or places to conceal them. Your passport, cash, and credit cards are most secure when locked in a hotel safe. When you have to carry them on your person, you may wish to conceal them in several places rather than putting them all in one wallet or pouch.

If you wear glasses, pack an extra pair. Bring them and any medicines you need in your carry-on luggage.

To avoid problems when passing through customs, keep medicines in their original, labeled containers. Bring a copy of your prescriptions and the generic names for the drugs. If a medication is unusual or contains narcotics, carry a letter from a doctor attesting to your need to take the drug. If you have any doubt about the legality of carrying a certain drug into a country, consult the embassy or consulate of that country first.

Bring travelers checks and one or two major credit cards instead of cash.

Put your name, address and telephone numbers inside and outside of each piece of luggage. Use covered luggage tags to avoid casual observation of your identity or nationality and if possible, lock your luggage.

SECTION III

WHILE IN A FOREIGN COUNTRY

GENERAL INFORMATION

Keep a low profile. Clothes and other outward signs of wealth or nationality should not be in stark contrast to those of the country in which you are traveling. Clothing should not give the impression of wealth or importance. If you are in the military, avoid wearing your uniform unless required.

Local banks usually offer better rates of exchange than hotels, restaurants, or stores. Rates are often posted in windows. Above all, deal only with authorized agents when exchanging currency. Exchanging money on the black market is illegal in many countries and can carry severe penalties. In some countries, you risk more than being swindled or stuck with counterfeit currency, you risk arrest.

Make a note of the credit limit on each credit card you carry. Make certain not to charge over that amount on your trip. In some countries travelers have been arrested for mistakenly exceeding their credit limit. Safeguard your credit cards and also the customer copy of each credit card transaction. Ask your credit card company how to report the loss of your card from abroad. [Your credit card's toll-free numbers do not work from abroad, but your company should have a number that you can call collect to report a lost or stolen card.](#) Always report the loss or theft of your credit cards or travelers checks immediately to the companies and notify the local police.

Some European countries levy a value added tax (VAT) on the items you buy. In some places, if you ship your purchases home, the VAT can be waived. Other places may require you to pay the VAT, but have a system to refund it to you by mail. Ask the store clerk for an application to apply for the refund. The VAT refund is only for items you can ship or carry with you. It does not apply to food, hotel bills, or other services. Because the rules for VAT refunds vary from country to country, check with the country's tourist office to learn the local requirements.

Be careful of the items you buy. Some items made from animals or plants, especially if made from endangered species, and many species of live animals cannot be brought into the U.S. legally. Your wildlife souvenirs could be confiscated by Government inspectors, and you could face penalties for attempting to bring them home. Also beware of purchasing glazed ceramic ware abroad for other than purely decorative purposes. If you consume food or beverages from improperly glazed ceramics there is a possibility of suffering from lead poisoning.

Some countries consider antiques to be national treasures. In some countries, customs authorities seize illegally purchased antiques without compensation and may also levy fines on the purchaser. Travelers have been arrested and prosecuted for purchasing antiques. Travelers have even been arrested for purchasing reproductions of antiques from street vendors because a local authority believed the purchase was an authentic antique. [In countries where antiques are important, protect yourself by documenting your purchases as reproductions if that is the case, or if they are authentic, secure the necessary export permit.](#)

Keep all receipts for items that you buy while traveling abroad. They will be helpful in filling out your U.S. customs declaration when you return.

LOCAL LAWS

The rights an American enjoys in this country do not travel abroad. Each country is sovereign and its laws apply to everyone who enters regardless of nationality. In many countries laws are similar to those in the U.S. However, laws in other countries may differ significantly. What may be legal or only a minor offense in the U.S. may be a major offense elsewhere.

[In some countries individuals are prohibited from making derogatory comments about the government or its leaders. Certain countries have very strict laws about the possession and use of alcohol. Some countries do not distinguish between possession and trafficking of drugs. Many countries have mandatory sentences even for possession of a small amount of marijuana or cocaine.](#)

Firearms, even those legally registered in the U.S., cannot be brought into a country unless a permit is first obtained from the embassy or a consulate of that country and the firearm is registered with foreign authorities on arrival. If you take firearms or ammunition to another country, you cannot bring them back into the U.S. unless you register them with U.S. Customs before you leave home.

Some countries are particularly sensitive about photographs. In general, refrain from photographing police and military installations and personnel; industrial structures including harbor, rail, and airport facilities; border areas; and scenes of civil disorder or other public disturbance.

Remember that when you leave the U.S., you are subject to the laws of the country where you are. Few countries provide a jury trial. Most countries do not accept bail. Pretrial detention often in solitary confinement may last months. Prisons may lack even minimal comforts such as a bed, toilet, or wash basin. Diets are often inadequate and require supplements from family or friends. Officials may not speak English. Physical abuse, confiscation of personal property, degrading or inhumane treatment, and extortion are possible.

The U.S. Government cannot get Americans released from foreign jails. When alerted, U.S. officials will visit you, advise you of your rights according to local laws, and contact your family or employer if you wish. They will do whatever they can to protect your legitimate interests and to ensure you are not discriminated against under local law. Consuls can transfer money, food, and clothing to the prison authorities from your family or friends. They will try to get relief if you are held under inhumane or unhealthy conditions or treated less favorably than others in your same situation.

PERSONAL SAFETY

On the Street

Use the same common sense traveling overseas that you would at home. Be especially cautious or avoid areas where you are likely to be victimized. Do not use short cuts, narrow alleys, or poorly lit streets. Avoid going out alone at night. Do not wander into areas that you would avoid if you were at home, such as dark alleys, hostile areas, etc.

Avoid public demonstrations and civil disturbances. Keep a low profile and avoid loud conversations or arguments. Do not discuss your travel plans or any other personal matters with strangers. Try to seem purposeful when you move about. Even if you are lost, act as if you know where you are going. When possible, ask directions only from individuals in authority. Learn how to use a pay telephone and have the proper change or token on hand.

Try to learn a few phrases in the local language that will enable you to call for emergency assistance. Also, carry emergency phone numbers with you, including the number of the nearest American embassy or consulate.

Avoid scam artists. Beware of strangers who approach you, offering bargains or to be your guide. Beware of pickpockets. They often have an accomplice who will jostle you, ask for directions or the time, point to something spilled on your clothing, or distract you by creating a disturbance. A child or even a woman carrying a baby can be a pickpocket. Beware of groups of children who create a distraction while picking your pocket.

If you are confronted, don't fight. Give up your valuables. Your money and passport can be replaced, but you cannot.

In the Hotel

Upon arrival at your hotel or temporary place of residence note emergency exits and have an exit plan in mind in the event of a fire or other emergency. Attempt to get a room on the second through seventh floors; above easy access by thieves, but low enough to be reached by fire equipment. Read the fire safety instructions in your hotel room. Know how to report a fire. Note the uniforms for hotel security and other hotel employees.

Be aware that foreign intelligence and security services sometimes search rooms; steal, photograph, or photocopy documents; download information from laptop computers; tap telephones; and/or install concealed listening devices. Never admit strangers into your room, no matter how plausible their story. Keep your hotel door locked at all times. Meet any visitors in the lobby. Do not leave any valuables in your hotel room while you are out; use the hotel safe.

Using Public Transportation

Use taxis that are clearly identified with official markings. Beware of unmarked cabs.

Robbery of passengers on trains is most common at night and especially on overnight trains. Do not accept food or drink from strangers. Lock your compartment if possible. If you must sleep in an unlocked and unprotected area, tie down your luggage, strap your valuables to you, and sleep on top of them as much as possible. Do not be afraid to alert authorities if you feel threatened in any way.

Use the same kind of caution on buses as you would on a train.

While Driving

If you rent a car, do not go for the exotic or flashy models. Choose a type commonly available locally. If possible, ask that markings identifying it as a rental car be removed.

Be sure the car is in good repair with universal door locks and power windows which give the driver better control of access to the car. An air conditioner is also a safety feature which allows you to drive with the windows closed.

Keep windows closed and doors locked. Do not leave valuables in the car. Never pick up hitchhikers. Do not get out of the car if you are uncomfortable with the area or if there are suspicious looking individuals nearby.

In some places, victimization of motorists has been refined to an art. Carjackers and thieves operate at gas stations, parking lots, in city traffic, and along the highway. Be suspicious of anyone who tries to get your attention when you are in or near the car.

In some areas, criminals use ingenious ploys. They may offer help, flag you down and ask for assistance or even try to drive you off the road or cause an accident. In other areas, criminals do not even waste time on ploys; they simply smash car windows at traffic lights, grab your valuables or your car, and get away. Defensive driving has come to mean more than avoiding accidents, it also means keeping an eye out for potential criminals on foot, on cycles, or on scooters.

Drive carefully. Some countries deal harshly with foreigners who are involved in traffic incidents. In some cases, drivers can be detained in jail while accidents are being investigated. Some countries impose fines for speeding that are payable on the spot. Some countries do not recognize U.S. drivers' licenses and only accept international drivers' licenses.

SECTION IV

TERRORISM AND INTELLIGENCE TARGETING

Terrorism

There are periods of time that terrorism may not seem to be a threat in a certain country, however, terrorist acts occur randomly and with unpredictably. The first and best protection is to avoid travel to unsafe areas where there has been a persistent record of terrorist attacks or kidnappings. The U.S. Department of State establishes Consular Information Sheets and Travel Warnings on current travel conditions in foreign countries. Current information may be obtained at www.travel.state.gov. or you can call 202-647-5225.

Before you travel, discuss with your family what they should do in the event of an emergency. Make sure that your affairs are in order before you leave home. If you leave a current will, insurance documents, and power of attorney with your family or a friend, you can feel secure about traveling and will be prepared for any emergency that may

arise while you are away. Find out if your personal property insurance covers you for loss or theft abroad. More important, check if your health insurance covers you abroad. Make sure your plan includes medical evacuation in the event of an accident or serious illness.

Just as a car thief will be attracted to an unlocked car with the key in the ignition, terrorists are looking for defenseless, easily accessible targets who follow predictable patterns. Try to schedule direct flights if possible. Minimize the time you spend in public areas at the airport; move quickly through the immigration and baggage claim areas. Do not browse or delay in the terminal area. Maintain a low profile and avoid actions that identify you as an American or someone who is wealthy or important.

Never leave your baggage unattended in airline terminals. Be observant, and if you see unattended or abandoned packages, briefcases, or baggage, leave the area promptly and report them to airport security or other authorities.

Never accept anything from strangers that they ask you to carry for them or deliver to someone residing in the U.S. This kind of request is sometimes used by intelligence operatives to entrap people by getting them to accept illegal items and are also used by criminals trying to smuggle goods into America.

If you travel by automobile, keep in mind that the majority of terrorist incidents are perpetrated against individuals while traveling in this manner. If you travel by taxi, choose your own cab at random. Do not ever take a vehicle that is not clearly identified as an official taxicab. Compare the face of the driver with the one posted on the license. If possible, travel with others.

If you are ever in a situation where somebody starts shooting, drop to the floor or get down as low as possible. Do not move until you are sure all danger has passed. Do not attempt to help rescuers, and do not pick up a weapon. Try to shield yourself behind or under a solid object and if you must move, crawl on your stomach.

If you ever find yourself in a hostage situation, remember that the most dangerous phases of a hijacking or hostage situation are the beginning and, if there is a rescue attempt, at the end. It is extremely important that you remain calm and manage your own behavior. Avoid resistance and any sudden or threatening movements. Do not struggle or try to escape. Try to remain inconspicuous and avoid eye contact or the appearance of observing the captors' actions or appearance. Put yourself in a mode of passive cooperation, and always comply with all orders and instructions. Breathe deeply and prepare yourself mentally, physically, and emotionally for the possibility of a long ordeal.

If you are involved in a lengthy situation maintain your sense of personal dignity and gradually increase your requests for personal comforts. Make any requests in a reasonable low-key manner. Do not be afraid to ask for anything you need or want, like medicines, books, pencils, papers, etc. Try to establish a rapport with your captors, but avoid any political discussions or other confrontational subjects. Eat whatever they give you, even if it does not look appetizing.

If questioned, keep your answers short and do not volunteer information. Talk normally, do not complain or get belligerent. Do not try to be a hero! Remember that you are a valuable commodity to your captors. It is important to them to keep you alive and well.

Intelligence Targeting

Dramatic geopolitical changes in the past few years have reshaped the threat posed to the United States by foreign intelligence services. Many foreign intelligence services today place a greater emphasis on the overt collection of information through unclassified sources. Usually, any intelligence activities directed against you will be conducted in an unobtrusive and non-threatening fashion. Many intelligence activities are conducted without the target even being aware of them. Common sense and basic counterintelligence awareness can effectively protect you against foreign attempts to collect sensitive, proprietary or other privileged information. Even a limited amount of information, classified or not, combined with information from other sources may give an advantage to foreign intelligence services.

Be careful what you discuss with strangers or what others, may overhear even in your own hotel room, which could have listening devices installed. Never use computer, facsimile, telex, or telephone equipment at foreign hotels or business centers for sensitive information. Keep sensitive material until it can be disposed of securely. Burn or shred paper and cut floppy disks in pieces to eliminate them. Keep your personal computer as carry-on baggage; never check it with other luggage.

If you suspect that a representative of a foreign intelligence service has approached you, report the details to your Security Office upon your return. If you decide that the contact should be reported immediately, report it to the Regional Security Officer or Post Security Officer at the nearest U.S. diplomatic facility and to your Security Office upon your return.

It is extremely important that you remain aware of what is going on around you. You are expected to report to your Security Office any observations you make or any information that you receive that would suggest that a foreign power may have knowledge of any U.S. national security information. The early identification and reporting of suspected foreign intelligence activities can help detect and neutralize a foreign intelligence operation.

Certification of Awareness
Foreign Travel Briefing & Contact Reporting Requirements
For FAA and Contractor Employees

I _____, (write/or type name and routing symbol)
certify that I have received and/or read this document before my foreign travel departure.

Signature

Date